IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:19-CR-130-MHL
	)	
OKELLO T. CHATRIE,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION FOR DISCOVERY OF SENSORVAULT DATA

The United States of America, by its undersigned attorneys, moves this Court to deny Defendant Okello T. Chatrie's motion for discovery of Google's "Sensorvault" data. (ECF No. 28).

The United States has disclosed every facet of data provided by Google, LLC ("Google"). Despite this complete disclosure, the defendant has filed a motion for discovery relating to Google's "Sensorvault" data, making far-reaching requests that give little to no regard for the contours of Federal Rule of Criminal Procedure 16 nor the Agreed Discovery Order entered in this case. The vast majority of the defendant's requests relate to documents and or information not in the United States' possession, custody, or control. For others, he fails to make a threshold showing of materiality warranting their disclosure.

To the extent that any of the requests are indeed discoverable, the United States will abide by the terms of the Agreed Discovery Order entered by this Court on October 1, 2019. (ECF No.15).

I. BACKGROUND

At approximately 4:50 p.m. eastern standard standard time, on May 20, 2019, a then-

unknown male entered the Call Federal Credit Union in Midlothian, Virginia with a firearm. While the man stood in line, victim-teller J.B. asked another teller, J.W., to assist this customer when he reached the counter. When he reached J.W.'s station, the man presented a handwritten note. That note read, in part, "I got your family as hostage and I know where you live, If you or your coworker alert the cops or anyone your family and you are going to be hurt . . . I need at least 100k." After J.W. told him that she did not have access to that amount of money, the armed robber pulled out a silver and black handgun. Waving the firearm around, he then directed J.W., other Call Federal Credit Union employees, and customers to move to the center of the lobby and get on the floor. Once there, the armed robber led victims behind the teller counter and into a back room where the Credit Union's safe was located.

Once in the back room, he ordered everyone to their knees at gunpoint and demanded that the bank manager open the safe. The Credit Union manager, fearing for his life, obliged by opening the safe and handing over $195,000 in United States currency.

After the armed robbery, victims dialed 911 to request assistance. When law enforcement arrived, they reviewed surveillance video from the credit union and determined that the armed robber entered the credit union from an area behind a nearby church, held a cellular telephone to his ear when entering the credit union, and ran back towards the church after the robbery. An employee of that church explained to law enforcement that he saw a suspicious individual in a newer model, blue Buick sedan prior to the time of the robbery.

With this information in hand, law enforcement sought and obtained a state search warrant on June 14, 2019, for information pertaining to anonymized accounts in the custody and control

of Google, Inc., identifying Google IDs[1] that were within the vicinity of the Call Federal Credit Union and the nearby church just prior to, and right after, the armed robbery. This search warrant is commonly referred to as a "GeoFence" warrant.[2]

Based on returns of information for 19 anonymized accounts from Google on June 28, 2019, law enforcement identified several accounts of interest. The lead case agent recognized at the outset that one particular Google ID (hereinafter, the "Chatrie Account") was likely the device involved in the armed robbery because, among other things, the Chatrie Account: (1) was near the church prior to the robbery at the same time that the church witness recalled seeing the suspicious individual in the dark blue Buick sedan; (2) was inside the credit union at the time of the robbery; and (3) immediately left the area following the robbery from an area near the church.

Pursuant to the state GeoFence search warrant, on July 10, 2019, Google provided additional location information and history for nine of the original nineteen anonymized Google IDs to account for thirty minutes before and thirty minutes after the armed robbery.

Based on a review of this additional location information, law enforcement discovered that the Chatrie Account traveled to XXXX Mason Dale Drive following the armed robbery. Law enforcement assessed XXXX Mason Dale Drive and found that a utilities inquiry showed the defendant listed as a subscriber for the Mason Dale address. Further database searches revealed that Chatrie was born in Jamaica, had purchased a silver and black nine millimeter G2C Taurus

[1] The information gleaned from Google pursuant to this search warrant was entirely anonymized through all but one phase—the final phase—of the returns for the warrant. More specifically, Google merely provided information associated with a "Device ID" number. Google explains that "the Device ID is used only for distinguishing unique devices in a particular user's location history and cannot be mapped to an Android ID or an IMEI/MEID."

[2] The United States provides a fuller rundown of the GeoFence warrant in its response in opposition to the defendant's motion to suppress the evidence obtained from that warrant.

semiautomatic firearm from Bob Moates Sports Shop less than one month before the armed robbery, and owned a blue, 2010 Buick Lacrosse. Virginia Employment Commission records showed Chatrie's most recent employment as The Home Depot. The Home Depot shared with law enforcement that Chatrie provided them with a home address of XXXX Mason Dale Drive, email address of okellochatrie55@gmail.com, and phone number of 804-475-8298 during the course of his employment with the home improvement store.

Pursuant to the GeoFence warrant, law enforcement then requested and obtained subscriber information for the Chatrie Account, and two additional anonymized accounts. On July 11, 2019, Google provided subscriber information for just these three accounts. The United States did not obtain any subscriber or other identifying information on the other 16 anonymized accounts. The subscriber information for the Chatrie Account had the email of okellochatrie55@gmail.com, a name of "Jamaican media," and showed a last login date of May 20, 2019, the date of the robbery of Call Federal Credit Union.

Law enforcement later obtained a federal search warrant on July 17, 2019, for historical location information for the Google account of okellochatrie55@gmail.com and Google account ID: 365520819283.[3] That location information demonstrated, among other things, that the account left XXXX Mason Dale Drive before the robbery and returned to XXXX Mason Dale Drive after the robbery.

Law enforcement also sought and obtained a federal search warrant on July 17, 2019, for historical and prospective location information from Sprint Mobile for the cellular telephone

[3] Importantly, the historical information obtained for Chatrie's account is the same type of information gleaned from the GeoFence warrant. That is, location information for Chatrie's Google account.

number 804-475-8298. It was later determined that the Sprint account for this phone number was deactivated on July 7, 2019.

On July 19, 2019, law enforcement sought and obtained federal search warrants, one for a cell site simulator to ascertain the defendant's new phone number[4] and another to place a tracking device on the defendant's 2010 blue Buick Lacrosse. At the same time, law enforcement obtained and analyzed toll records from Sprint for the defendant's phone, his father's phone, and his sister's phone. Analysis of the defendant's father's and sister's toll records revealed a telephone number in common that was later discovered to belong to the defendant, despite having someone else listed as the subscriber for the T-Mobile telephone.

Law enforcement also surveilled the defendant beginning in mid-July. Surveillance of the defendant and his vehicle revealed that he spent the vast majority of his time at XXXX Willis Street and XXX Rosegill Road.

Further review of the historical location information obtained from the federal search warrant obtained on July 17, 2019, showed that the defendant spent much of his time at XXXX Mason Dale Drive during the week prior to the robbery, was near the Call Federal Credit Union at the time of the robbery, was near XXXX Mason Dale Drive before and after the robbery, and spent several hours at XXX Rosegill Road. During the week following the armed robbery, the defendant's phone was located at XXXX Mason Dale Drive and the Rosegill residence. Law enforcement surveillance between July 23, 2019, and August 12, 2019, revealed that the defendant spent most of his evenings at XXXX Willis Street.

On August 12, 2019, law enforcement sought and obtained a search warrant for the

[4] No evidence of value was obtained from the use of the cell site simulator.

residences located at XXXX Mason Dale Drive, XXXX Willis Street, XXX Rosegill Road, and the Buick Lacrosse. When executing these search warrants in the early morning of August 13, 2019, law enforcement recovered evidence of value from XXXX Mason Dale Drive and XXXX Willis Street. At the XXXX Mason Dale Drive residence, law enforcement recovered two robbery-style demand notes from the bedroom belonging to the defendant. At XXXX Willis Street, law enforcement recovered nearly $100,000 in United States Currency (including bills wrapped in bands signed by the victim-bank teller), a silver and black firearm that appeared to be identical to the firearm used in the robbery, a money counter, and a safe.[5]

The defendant was at XXXX Willis Street when the search warrant was executed. After being placed under arrest and advised of his *Miranda* rights, the defendant admitted to the armed robbery of the Call Federal Credit Union on May 20, 2019.

On September 17, 2019, a Richmond grand jury returned a two-count indictment for Forced Accompaniment during an Armed Credit Union Robbery, in violation of 18 U.S.C. § 2113(e), and Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A)(i). The defendant pleaded not guilty on October 1, 2019, and trial was scheduled for December 3, 2019, through December 5, 2019, at 9:00 a.m. before the Honorable M. Hannah Lauck. At a status conference, on November 12, 2019, the Court granted the defendant's motion to continue trial beyond the speedy trial date. (ECF No. 34)

On October 22, 2019, the defendant filed the Motions to Suppress that are subject of this response.

[5] All electronics recovered—whether cellular telephones or computers—returned no evidence of value. Moreover, the defendant and his girlfriend provided consent to search the cellular telephones and computers recovered from XXXX Willis Street.

II. ARGUMENT

Federal Rule of Criminal Procedure 16 provides, in relevant part, that the United States must turn over certain "items, if the item is within the government's possession, custody, or control." Fed. R. Crim. P. 16(a)(1)(E). The Fourth Circuit stated it rather matter-of-factly, observing that "the government cannot disclose what it does not have." *United States v. Shambari*, 484 F.2d 931, 935 (4th Cir. 1973); *see also United States v. Pinto*, 905 F.2d 47, 50 (4th Cir. 1990) ("Rule 16(a)(1)(C) 'triggers the government's disclosure obligation only with respect to documents within the federal government's actual possession, custody, or control.'").

Even where the items are in the United States' possession, custody, or control, there is only an obligation to turn over items "material to preparing the defense," intended for use in the United States' case-in-chief at trial, or "obtained from or belong[ing] to the defendant." *See* Fed. R. Crim. 16(a)(1)(E). In assessing materiality, the burden is on the defendant to show "that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor." *United States v. Caro*, 597 F.3d 608, 621 (4th Cir. 2010). The defendant must make some showing as to how the discovery "would have actually helped prove his defense." *Id.* at 621; *see also United States v. White*, No. 15-6193, 2016 WL 2989567, *4 (D. Md. May 24, 2016) ("The Fourth Circuit thus requires the defendant to present facts showing that the requested information will actually help prove his defense, not merely that it might help prove his defense."); *United States v. Matish*, 193 F. Supp. 3d 585, 601 (E.D. Va. 2016) ("Notably, the purposes for which Defendant asks for access to the missing source code are based upon speculation as to what the declarants might find . . . Such speculation remains insufficient to serve as a basis to compel discovery.").

As an initial matter, the United States has provided the defendant with every item obtained

from Google pursuant to the Google GeoFence search warrant. Despite this reality, the defendant now requests:

> (1) the location/source of the WiFi access points for individuals' location tracking data listed as "WiFi" in the "source" section of certain spreadsheets produced; (2) the anonynmous identifier used for the defendant's sensorvault data; (3) details concerning Google's Sensorvault Data; (4) Parameters of Google's Sensorvault data, including how many individuals' tracking information is in the Sensorvault; (5) The name(s) and training, certifications, and qualifications of the individual(s) at Google who gathered and turned over the location data in this case to law enforcement officials; and (6) Any and all Sensorvault data that Google initially determined to be potentially responsive to the warrant and subsequent law enforcement requests but excluded from the Sensorvault data ultimately Google provided to law enforcement officials in this case, including the reason(s) for the exclusion

Def.'s Mot. to Suppress at 1-4, ECF No. 28.

The United States does not have access to these items because they have not been produced pursuant to a search warrant obtained in this investigation and, as such, remain in the possession, custody, and control of Google. Notably, the defendant has been provided with the email address, business address, and names of the Google employees who have supplied the information to the United States pursuant to these search warrants.[6] *See United States v. Cameron*, 672 F. Supp. 2d 133, 138 (D. Me. 2009) ("Although the servers and/or server files are 'tangible objects' within the meaning of Rule 16(a)(1)(E), the Government maintains that these items are not within its possession, custody, or control, and the Government has provided the Defendant with the names

[6] Federal Rule of Criminal Procedure 17(c) provides the defendant with compulsory process through which to "order the witness to produce any books, papers, documents, data, or other objects the subpoena designates." Fed. R. Crim. P. 17(c); *see also United States v. Rand*, 835 F.3d 451, 463 (4th Cir. 2016); *United States v. Llanez-Garcia*, 735 F.3d 483, 494 (6th Cir. 2013); *Bowman Dairy Co. v. United States*, 341 U.S. 214, 219 (1951) (observing that there is "[n]o good reason" why documents not subject to Rule 16 "may not be reached by subpoena under Rule 17(c) as long as they are evidentiary").

and business addresses for Yahoo!'s in-house general counsel, its compliance director, and its compliance paralegal to allow Mr. Cameron, should he desire to do so, to contact Yahoo! and directly obtain these tangible items.").

The defendant's request for the training, certifications, and qualifications of these individuals again disregards the discovery obligations set forth in Rule 16. Such information is plainly not within the possession, custody, or control of the United States. *See id.* at 138–39 n.4 (rejecting defendant's motion for additional discovery from the United States requesting "[n]ames, addresses and dates of birth of any Yahoo! [e]mployee who identified or reviewed potential illegal images, or who transmitted (including electronically) information and images referenced in discovery to NCMEC . . . or who handled any of the said preserved or recorded data, including but not limited to support staff, mailroom employees, or messengers.").

With respect to the other requests, the United States has already provided much of the information. Specifically, the United States has provided: (1) anonymous identifier used for Mr. Chatrie's Sensorvault data in this case; (2) copies of the raw data produced by Google and utilized by law enforcement; (3) arrest and investigative reports from any officers/analysts who used the Sensorvault data during this case; and (4) communications and correspondence between agents involved in the investigation and Google employees/representatives regarding the Sensorvault data in this case.

The defendant's request for information about how law enforcement officials manipulated and analyzed the data received from Google to identify relevant anonymized accounts for the second and third phase of the GeoFence warrant seeks to impose greater obligations upon the United States than those provided for under the Agreed Discovery Order. The United States will abide by its expert notice obligations and will make available any summary evidence that to be

presented at the Motion to Suppress hearing or at trial of this matter.

The defendant's remaining requests do not relate to items obtained from or belonging to the defendant nor items intended for use in the United States' case-in-chief at trial. Accordingly, the defendant must demonstrate that these items are "material to preparing [his] defense." Fed. R. Crim. P. 16(a)(1)(E)(iii). He fails to do so.

In particular, he does not demonstrate the materiality of physical access to any and all devices and software used in this case by any federal, state or local law enforcement official to manipulate and analyze the Sensorvault data; training materials in the possession of law enforcement agencies for obtaining and using Sensorvault data; and contracts, memorandums of understanding and agreements, including but not limited to nondisclosure agreements, concerning the use of Sensorvault data, or that bind the law enforcement agencies. *See, e.g.*, *United States v. Losch*, No. CR-19-00294-001-PHX-MTL, 2019 WL 5420549, *5 (D. Ariz. Oct. 23,2019) (denying motion for discovery of training instructions and manuals from law enforcement agencies where defendant failed to demonstrate materiality). Notably, the Federal Bureau of Investigation agents in this case indicate that such information, particularly training materials and contacts on the use of "Sensorvault" data, do not appear to exist. Moreover, the call for physical access to any and all devices and software used in this case likely will reach an area of law enforcement investigative techniques that are protected from disclosure.[7]

The defendant fails to show materiality for the aforementioned items because quite frankly these requests lack little, if any, connection to his guilt or innocence in this case. In other words, nary a contract, policy, or device of the Federal Bureau of Investigation will "alter the quantum of

[7] At this time, the only "software" utilized by law enforcement to assess data produced by Google appears to be both Microsoft Excel and Google Earth.

proof in [the defendant's] favor." *United States v. Caro*, 597 F.3d at 621. In *Caro*, the Fourth Circuit affirmed a district court's denial of a defendant's request for discovery during the death penalty phase of his case. In doing so, the Fourth Circuit made clear that materiality does not turn on relevance—rather, the question is whether the information "would have actually helped prove his defense":

> The information was relevant to future dangerousness and might have allowed Cunningham to formulate scientifically more reliable opinions about Caro and to test various government allegations, e.g., that gang membership made Caro more dangerous. However, Caro presented no facts whatsoever indicating that the information would have actually helped prove his defense. *See United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990) ("Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense.").

Id.

That is the burden the defendant bears and he fails to provide a single argument on why these items are at all material to his defense against the charges in the indictment. None of them will call into question the underlying GPS coordinates provided by Google in identifying the defendant's device. To the extent the defendant has qualms with the United States' analysis of the underlying data provided by Google, they have full and equal access to that data. They may, and presumably will, dissect the coordinates provided by Google.

The data disclosed by Google is in the defendant's possession. He will, of course, gain access to evidence prepared by the United States using those disclosed latitude and longitude coordinates. Importantly, the information provided under the GeoFence warrant is comprised of latitude and longitude coordinates and the source of those coordinates (*i.e.*, GPS or Wi-Fi) for anonymized accounts responsive to the metes and bounds of the search warrant.

III. CONCLUSION

The Court should deny the defendant's motion to for discovery.

Respectfully submitted,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 19th day of November, 2019, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koenig
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
Assistant United States Attorney
Office of the United States Attorney
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov